日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１２月１８日

出願番号
Application Number: 特願２００２－３６６２５８

[ST.10/C]: [ＪＰ２００２－３６６２５８]

出願人
Applicant(s): 株式会社山武

２００３年　７月　４日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５３４６８

【書類名】　特許願
【整理番号】　20020318
【提出日】　平成14年12月18日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
　【氏名】　三島　崇
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
　【氏名】　佐内　大司
【特許出願人】
　【識別番号】　000006666
　【氏名又は名称】　株式会社　山武
【代理人】
　【識別番号】　100095072
　【弁理士】
　【氏名又は名称】　岡田　光由
　【電話番号】　03-3807-1818
【手数料の表示】
　【予納台帳番号】　012944
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9722522

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　パスワード作成方法及びパスワード作成プログラム

【特許請求の範囲】

【請求項１】　作成対象となるパスワードの生成順番の情報を入力する過程と、

パスワード推測ツールで用いられるものと同一の生成手順に従って平文のパスワード候補を生成するパスワード候補生成ルーチンを使って、そのパスワード候補生成ルーチンが上記生成順番の所で生成するパスワード候補を取得する過程と、

上記取得したパスワード候補を作成対象のパスワードとして出力する過程とを備えることを、

特徴とするパスワード作成方法。

【請求項２】　作成対象となるパスワードの強度を示す情報を入力する過程と、

上記強度を示す情報を、パスワード推測ツールで用いられるものと同一の生成手順に従って平文のパスワード候補を生成するパスワード候補生成ルーチンが生成することになるパスワード候補の生成順番の情報に変換する過程と、

上記パスワード候補生成ルーチンを使って、上記パスワード候補生成ルーチンが上記生成順番の所で生成するパスワード候補を取得する過程と、

上記取得したパスワード候補を作成対象のパスワードとして出力する過程とを備えることを、

特徴とするパスワード作成方法。

【請求項３】　請求項１又は２記載のパスワード作成方法において、

上記取得する過程では、上記生成順番の近傍でランダムにその値を変更することで１つ又は複数の生成順番を作成して、上記生成順番に加えて、あるいは上記生成順番に代えて、その作成した生成順番の所で生成されるパスワード候補を取得することを、

特徴とするパスワード作成方法。

【請求項４】　請求項１ないし３のいずれか１項に記載のパスワード作成方

法において、

上記出力する過程では、上記取得したパスワード候補が過去に出力したパスワードと一致するのか否かを判断して、一致しないことを条件にして、上記取得したパスワード候補を作成対象のパスワードとして出力することを、

特徴とするパスワード作成方法。

【請求項５】　請求項１ないし４のいずれか１項に記載のパスワード作成方法において、

上記出力する過程では、上記取得したパスワード候補が辞書に登録されている単語と一致するのか否かを判断して、一致しないことを条件にして、上記取得したパスワード候補を作成対象のパスワードとして出力することを、

特徴とするパスワード作成方法。

【請求項６】　作成対象となるパスワードの生成順番の情報を入力する処理と、

パスワード推測ツールで用いられるものと同一の生成手順に従って平文のパスワード候補を生成するパスワード候補生成ルーチンを使って、そのパスワード候補生成ルーチンが上記生成順番の所で生成するパスワード候補を取得する処理と、

上記取得したパスワード候補を作成対象のパスワードとして出力する処理とをコンピュータに実行させるためのパスワード作成プログラム。

【請求項７】　作成対象となるパスワードの強度を示す情報を入力する処理と、

上記強度を示す情報を、パスワード推測ツールで用いられるものと同一の生成手順に従って平文のパスワード候補を生成するパスワード候補生成ルーチンが生成することになるパスワード候補の生成順番の情報に変換する処理と、

上記パスワード候補生成ルーチンを使って、上記パスワード候補生成ルーチンが上記生成順番の所で生成するパスワード候補を取得する処理と、

上記取得したパスワード候補を作成対象のパスワードとして出力する処理とをコンピュータに実行させるためのパスワード作成プログラム。

【請求項８】　請求項６又は７記載のパスワード作成プログラムにおいて、

上記取得する処理では、上記生成順番の近傍でランダムにその値を変更することで１つ又は複数の生成順番を作成して、上記生成順番に加えて、あるいは上記生成順番に代えて、その作成した生成順番の所で生成されるパスワード候補を取得することを、

特徴とするパスワード作成プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、パスワードを作成するパスワード作成方法と、そのパスワード作成方法の実現に用いられるパスワード作成プログラムとに関し、特に、強さの保証されたパスワードを作成できるようにするパスワード作成方法と、そのパスワード作成方法の実現に用いられるパスワード作成プログラムとに関する。

【０００２】

【従来の技術】

ユーザがコンピュータ上で動作するシステムを利用する場合には、ユーザに対して、予めコンピュータに登録させたパスワードと同一のパスワードを入力させるようにすることで、ユーザがシステムを利用できる本人であるのか否かを確認するようにしている。

【０００３】

コンピュータに登録されるパスワードは、盗まれる可能性があることから暗号化されており、これから、システムの利用時にユーザから平文のパスワードが入力されると、それを暗号化して、この登録されている暗号化パスワードと一致するのか否かを判断することで、ユーザがシステムを利用できる本人であるのか否かを確認するようにしている。

【０００４】

ところで、人間が作り出すパスワードは何らかの規則性が出ることが多く、脆弱なパスワードとなりやすい傾向がある。

【０００５】

そこで、従来では、強度の要求されるパスワードを付ける必要がある場合には

、パスワード生成ツールにより自動生成されたパスワードを付けるようにしている。

【０００６】

【発明が解決しようとする課題】

しかしながら、これまでに用いられているパスワード生成ツールは、単なるランダム性に基づいてパスワードを生成する方法を用いており、これから、必ずしも強いパスワードとはならないことがある。

【０００７】

すなわち、従来のパスワード生成ツールを用いていると、人間が作り出すパスワードのような何らかの規則性が出るということはないものの、単なるランダム性に基づいてパスワードを生成する方法を用いていることから、必ずしも強いパスワードとはならないことが起こるのである。

【０００８】

本発明はかかる事情に鑑みてなされたものであって、強さの保証されたパスワードを作成できるようにする新たなパスワード作成技術の提供を目的とする。

【０００９】

【課題を解決するための手段】

本発明者らは、先に出願した特願２００２－２９８１９０で、数値的に表現されるパスワードの強度を実用的な時間内に算出できるようにする新たなパスワード強度検査技術を提案した。

【００１０】

この特願２００２－２９８１９０で開示した発明では、パスワードに対するブルートフォース攻撃に耐えられる時間の長さを測定することで、パスワードの強度を得るようにしている。

【００１１】

ブルートフォース攻撃では、図１０に示すように、パスワードとして使用できるすべての文字を組み合わせることで平文のパスワード候補を生成して、それを暗号化したものがコンピュータに登録されている暗号化パスワードと一致するのか否かについて判断することを繰り返していくことで、その暗号化パスワードに

対応付けられる平文のパスワードを盗み取るようにしている。

【００１２】

このブルートフォース攻撃に用いられるパスワード推測ツールとして、最近では、効率的なブルートフォース攻撃を行うために、文字の出現頻度の統計情報に基づいてパスワード候補を生成する「Ｊohn the Ｒipper」のようなパスワード推測ツールが用いられている（三島など:"ブルートフォースに勝つ“強いパスワード”とは",日経ネットワークセキュリティ,Vol.2,pp.36-47(2002)）。

【００１３】

特願２００２－２９８１９０で開示した発明では、このような文字の出現頻度の統計情報に基づいてパスワード候補を生成する「Ｊohn the Ｒipper」などのようなパスワード推測ツールを想定して、検査対象のパスワードがそのパスワード推測ツールの何番目に生成されるのか（ブルートフォース攻撃に耐えられる時間の長さに対応付けられる）を特定することで、検査対象のパスワードの強度を測定するようにしている。

【００１４】

この測定にあたって、特願２００２－２９８１９０で開示した発明では、検査対象のパスワードの強度測定を実用的な時間内に実現するために、パスワード推測ツールの生成した暗号化前のパスワード候補と検査対象の平文のパスワードとを照合することで、検査対象のパスワードの強度を測定するようにしている。

【００１５】

本発明では、特願２００２－２９８１９０で開示した発明で得られるパスワードの強度がパスワード推測ツールで生成されるパスワード候補の生成順番に対応付けられることに着目して、ユーザに対して、そのようなパスワードの強度を入力させるようにして、その入力させたパスワードの強度に対応付けられる生成順番を求めて、それに基づいて、パスワード推測ツールを使ってパスワードを作成するという構成を採る。

【００１６】

また、本発明では、特願２００２－２９８１９０で開示した発明で得られるパスワードの強度がパスワード推測ツールで生成されるパスワード候補の生成順番

に対応付けられることに着目して、ユーザに対して、そのようなパスワード候補の生成順番の情報を入力させるようにして、その入力させた生成順番に基づいて、パスワード推測ツールを使ってパスワードを作成するという構成を採る。

【００１７】

この構成に従って、本発明によれば、例えば２年間はブルートフォース攻撃に耐えられるというような強さの保証されたパスワードを作成できるようになる。これから、ユーザは、安心してパスワードを使うことができるようになる。

【００１８】

【発明の実施の形態】

以下、実施の形態に従って本発明を詳細に説明する。

【００１９】

図１に、本発明を具備するパスワード作成支援装置１の一実施形態例を図示する。

【００２０】

この図に示す本発明を具備するパスワード作成支援装置１は、検査対象のパスワードの強度を測定したり、指定される強度を持つパスワードを作成する処理を行うものであって、ユーザとの対話手段となる入出力装置１０と、「Ｊohn the Ripper」などのようなパスワード推測ツールで用いられて、平文のパスワード候補を生成するパスワード候補生成ルーチン１１と、パスワード候補生成ルーチン１１を使って検査対象のパスワードの強度を検査するパスワード強度検査プログラム１２と、本発明を実現すべく用意されて、パスワード候補生成ルーチン１１を使って強さの保証されたパスワードを作成するパスワード作成プログラム１３と、パスワード作成プログラム１３の作成したパスワードを記録する出力履歴テーブル１４と、パスワードとして用いられる可能性のある単語情報を蓄積する単語辞書１５とを備える。

【００２１】

ここで、本発明を実現すべく用意されるパスワード作成プログラム１３は、半導体メモリなどの記録媒体に記録して提供されたり、ネットワークを介して提供されることになる。

【００２２】

このパスワード作成プログラム１３は、後述する処理フローから分かるように、作成するパスワードの強度の情報を入力する機能と、入力した強度の情報をパスワード候補生成ルーチン１１の生成するパスワード候補の生成順番の情報に変換する機能と、パスワード候補生成ルーチン１１を制御することで強さの保証されたパスワードを作成する機能と、出力履歴テーブル１４や単語辞書１５を検索する機能と、作成したパスワードを出力する機能とを有する。

【００２３】

パスワード候補生成ルーチン１１は、「Ｊohn the Ｒipper 」などのようなパスワード推測ツールで用いられて、例えば、最初は、辞書に記載された文字列を使って平文のパスワード候補を生成し、続いて、パスワードとして使用できるすべての文字列を使って平文のパスワード候補を生成していくことで、７兆を超える平文のパスワード候補を規定の順番に従って生成するように処理する。

【００２４】

次に、図２に示す処理フローに従って、パスワード強度検査プログラム１２の実行する処理について説明する。

【００２５】

パスワード強度検査プログラム１２は、入出力装置１０から検査対象のパスワードを指定して、そのパスワードの強度の検査要求が発行されると、図２の処理フローに示すように、先ず最初に、ステップ１０で、その検査対象のパスワードを入力し、続くステップ１１で、パスワード候補生成ルーチン１１に対して、パスワード候補の生成を指示する。

【００２６】

このパスワード候補の生成指示を受け取ると、パスワード候補生成ルーチン１１は、パスワード推測ツールで用いられるときと同様の手順に従って、今回初めてパスワード候補を生成するときには、最初のパスワード候補（平文）を生成し、前回パスワード候補を生成しているときには、前回生成したパスワード候補に続くパスワード候補（平文）を１つ生成する。

【００２７】

これから、続いて、ステップ１２で、パスワード候補生成ルーチン１１から、その生成されたパスワード候補を受け取り、続くステップ１３で、入力したパスワードとその受け取ったパスワード候補とが一致するのか否かを判断する。

【００２８】

この判断処理により、入力したパスワードとパスワード候補生成ルーチン１１から受け取ったパスワード候補とが一致しないことを判断するときには、ステップ１４に進んで、これまでに受け取ったパスワード候補の個数と、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数とが一致したのか否かを判断して、一致しないことを判断するときには、次のパスワード候補の生成を指示すべくステップ１１に戻る。

【００２９】

このようにしてステップ１０～１４の処理を繰り返していくことで、ステップ１３で、入力したパスワードとパスワード候補生成ルーチン１１から受け取ったパスワード候補とが一致することを判断したり、あるいは、ステップ１８で、これまでに受け取ったパスワード候補の個数とパスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数とが一致したことを判断すると、ステップ１５に進んで、これまでに受け取ったパスワード候補の個数と、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数との比率値ｔ（０≦ｔ≦１）

ｔ＝（パスワード候補生成個数）／（パスワード候補最大生成可能個数）

を算出する。

【００３０】

続いて、ステップ１６で、

得点＝１００×ｔ

の算出式に従って、入力したパスワードの強度を示す得点を算出し、続くステップ１７で、

推定解析時間＝τ×（生成したパスワード候補の個数）

の算出式に従って、悪意のあるユーザがパスワード推測ツールを使って入力したパスワードをブルートフォース攻撃をしたときに要する解析時間を推定する。

【００３１】

ここで、τは、１個のパスワード候補を生成してハッシュ化（暗号化）し、それをブルートフォース攻撃対象の暗号化パスワードと比較して、両者が一致するのか否かを判断するまでの処理を行うのに要する時間を示している。

【００３２】

そして、最後に、ステップ１８で、入力した検査対象のパスワードの強度情報として、算出した得点および推定解析時間を入出力装置１０に出力して、処理を終了する。

【００３３】

このようにして、パスワード強度検査プログラム１２は、検査対象のパスワードがブルートフォースの攻撃で用いられるパスワード推測ツールで生成される平文のパスワード候補の何個目のパスワードに該当するのかということを測定して、その何個目という数に従ってパスワードの強度を決定して出力するように処理するのである。

【００３４】

本発明を実現すべく用意されるパスワード作成プログラム１３は、ユーザに対して、パスワード強度検査プログラム１２により算出される推定解析時間に相当する時間を入力させて、その時間に該当する推定解析時間を強度として持つパスワードを作成することで、例えば２年間はブルートフォース攻撃に耐えられるというような強さの保証されたパスワードを作成して出力する処理を行う。

【００３５】

次に、図３に示す処理フローに従って、このパスワード作成プログラム１３の実行する処理について詳細に説明する。

【００３６】

パスワード作成プログラム１３は、入出力装置１０のディスプレイに、図４に示すようなパスワード強度の入力域を持つパスワード作成入力画面を表示しているときに、ユーザから、その入力域に対してパスワード強度となる時間を入力してパスワードの作成要求が発行されると、図３の処理フローに示すように、先ず最初に、ステップ２０で、そのパスワード強度となる時間（年数日数）を入力す

る。

【００３７】

続いて、ステップ２１で、その入力した時間を上述のτで割り算することで、その入力した時間をパスワード候補生成ルーチン１１が生成するパスワード候補の順番に変換する。

【００３８】

すなわち、上述したように、

推定解析時間＝τ×（生成したパスワード候補の個数）

という関係式があることから、この関係式に従って、入力した時間をτで割り算することで、パスワード候補生成ルーチン１１が生成するパスワード候補の生成順番（以下、N_0 と記載する）に変換するのである。

【００３９】

続いて、ステップ２２で、その生成順番N_0 の近傍で、ｍ個の生成順番N_1 ～N_m をランダムに発生し、続くステップ２３で、生成順番N_i （ｉ＝０～ｍ）の指定に用いる変数ｉに０をセットする。

【００４０】

続いて、ステップ２４で、パスワード候補生成ルーチン１１に対して、生成順番N_i のパスワード候補の生成を指示する。

【００４１】

この指示を受け取ると、パスワード候補生成ルーチン１１は、図５に示すように、生成順番N_i の生成手順位置を検出して、そこにおけるパスワード候補を生成して返してくる。

【００４２】

これから、続いて、ステップ２５で、パスワード候補生成ルーチン１１から、生成順番N_i の所で生成されたパスワード候補を受け取る。

【００４３】

続いて、ステップ２６で、その受け取ったパスワード候補が単語辞書１５に登録されているのか否かを判断して、単語辞書１５に登録されていないことを判断するときには、ステップ２７に進んで、その受け取ったパスワード候補が出力履

歴テーブル１４に記録されているのか否かを判断することで、既に出力済みであるのか否かを判断する。

【００４４】

このステップ２７の判断処理により、パスワード候補生成ルーチン１１から受け取ったパスワード候補が出力済みでないことを判断するときには、ステップ２８に進んで、その受け取ったパスワード候補を出力対象として設定してから、ステップ２９に進んで、変数ｉの値を１つインクリメントする。

【００４５】

一方、ステップ２６で、受け取ったパスワード候補が単語辞書１５に登録されていることを判断するときと、ステップ２７で、受け取ったパスワード候補が出力済みであることを判断するときには、パスワードとして使用することは適切でないので、ステップ２８の処理を省略し、直ちにステップ２９に進んで、変数ｉの値を１つインクリメントする。

【００４６】

続いて、ステップ３０で、変数ｉの値がｍよりも大きくなったのか否かを判断して、変数ｉの値がｍよりも大きくなっていないことを判断するときには、次の生成順番N_iに対しての処理を行うべくステップ２４に戻り、変数ｉの値がｍよりも大きくなったことを判断するときには、ステップ３１に進んで、出力対象として設定したパスワード候補を出力履歴テーブル１４に登録してから入出力装置１０に出力して、処理を終了する。

【００４７】

このようにして、パスワード作成プログラム１３は、図４に示すようなパスワード作成入力画面に例えば２年間という時間を指定してパスワードの作成要求が発行されると、２年間はブルートフォース攻撃に耐えられる例えば１０個のパスワード候補を作成して、それを図６に示すように出力するように処理するのである。

【００４８】

これから、ユーザは、長い時間ブルートフォース攻撃に耐えられるパスワードを必要とするときには、パスワード作成入力画面に対して長い時間を入力するだ

けで、そのようなパスワードを入手することができるようになる。

【００４９】

ただし、長い時間ブルートフォース攻撃に耐えられるパスワードは、通常使用しないような記号が多く用いられることになるので、ユーザは、文字や数字が多く用いられるような記憶しやすいパスワードが欲しいときには、両方を勘案してパスワード作成入力画面に対してそれなりの時間を入力することになる。

【００５０】

ここで、図３の処理フローでは、生成順番N_0の所で生成されたパスワード候補についても出力対象に含める形で説明したが、ステップ２３の処理で変数ｉに１をセットすることで、このようなパスワード候補については出力対象から除外するようにしてもよい。

【００５１】

また、図３の処理フローでは、パスワード候補生成ルーチン１１は、生成順番N_iを受け取ると、その生成順番N_iの所におけるパスワード候補をいわば一発で生成できるという機能を持っていることで説明したが、そのような機能を持たない場合には、図７に示すように、パスワード作成プログラム１３が、パスワード候補生成ルーチン１１に対して繰り返しパスワード候補の生成を依頼していくことで、生成順番N_iの所で生成されたパスワード候補を取得するようにしてもよい。

【００５２】

また、図３の処理フローでは、ユーザに対して、パスワード強度となる時間を入力させるようにしているが、この時間の代わりに、生成順番N_0を直接入力させるようにしてもよい。

【００５３】

この場合には、パスワード作成プログラム１３は、図３の処理フローに代えて、図８の処理フロー（図３の処理フローのステップ２０～２２に代えて、ステップ５０～５１を実行する処理フロー）を実行することになる。

【００５４】

また、図３の処理フローでは、パスワード強度として時間を入力させるように

しているが、図２の処理フローで求められる得点のようなその他の情報をパスワード強度として入力させるようにしてもよい。

【００５５】

また、パスワード作成プログラム１３は、図３の処理フローに代えて、図９の処理フローを実行するようにしてもよい。この処理フローに従う場合には、パスワード強度の入力に応答して、常にｍ個のパスワード候補を作成して出力するように動作することになる。

【００５６】

【発明の効果】

以上説明したように、本発明によれば、例えば２年間はブルートフォース攻撃に耐えられるというような強さの保証されたパスワードを作成できるようになる。

【００５７】

これから、本発明によれば、ユーザは、安心してパスワードを使うことができるようになる。

【図面の簡単な説明】

【図１】

本発明を具備するパスワード作成支援装置の一実施形態例である。

【図２】

パスワード強度検査プログラムの実行する処理フローである。

【図３】

パスワード作成プログラムの実行する処理フローである。

【図４】

パスワード作成入力画面の説明図である。

【図５】

パスワード候補生成ルーチンの実行する処理の説明図である。

【図６】

パスワード作成入力画面の説明図である。

【図７】

パスワード作成プログラムの実行する処理の説明図である。

【図８】

パスワード作成プログラムの実行する処理フローである。

【図９】

パスワード作成プログラムの実行する処理フローである。

【図１０】

ブルートフォース攻撃の説明図である。

【符号の説明】

１　　パスワード作成支援装置

１０　入出力装置

１１　パスワード候補生成ルーチン

１２　パスワード強度検査プログラム

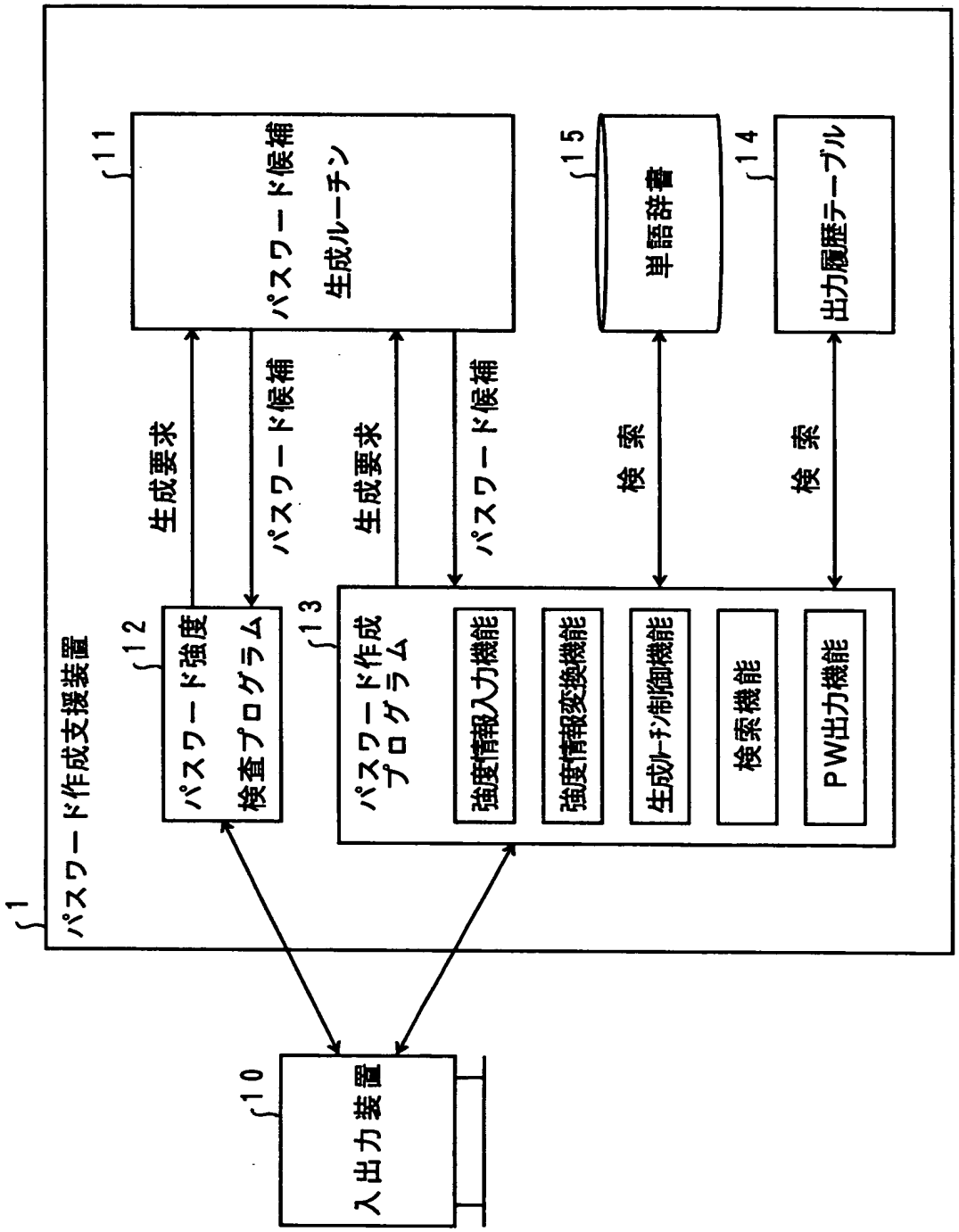
１３　パスワード作成プログラム

１４　出力履歴テーブル

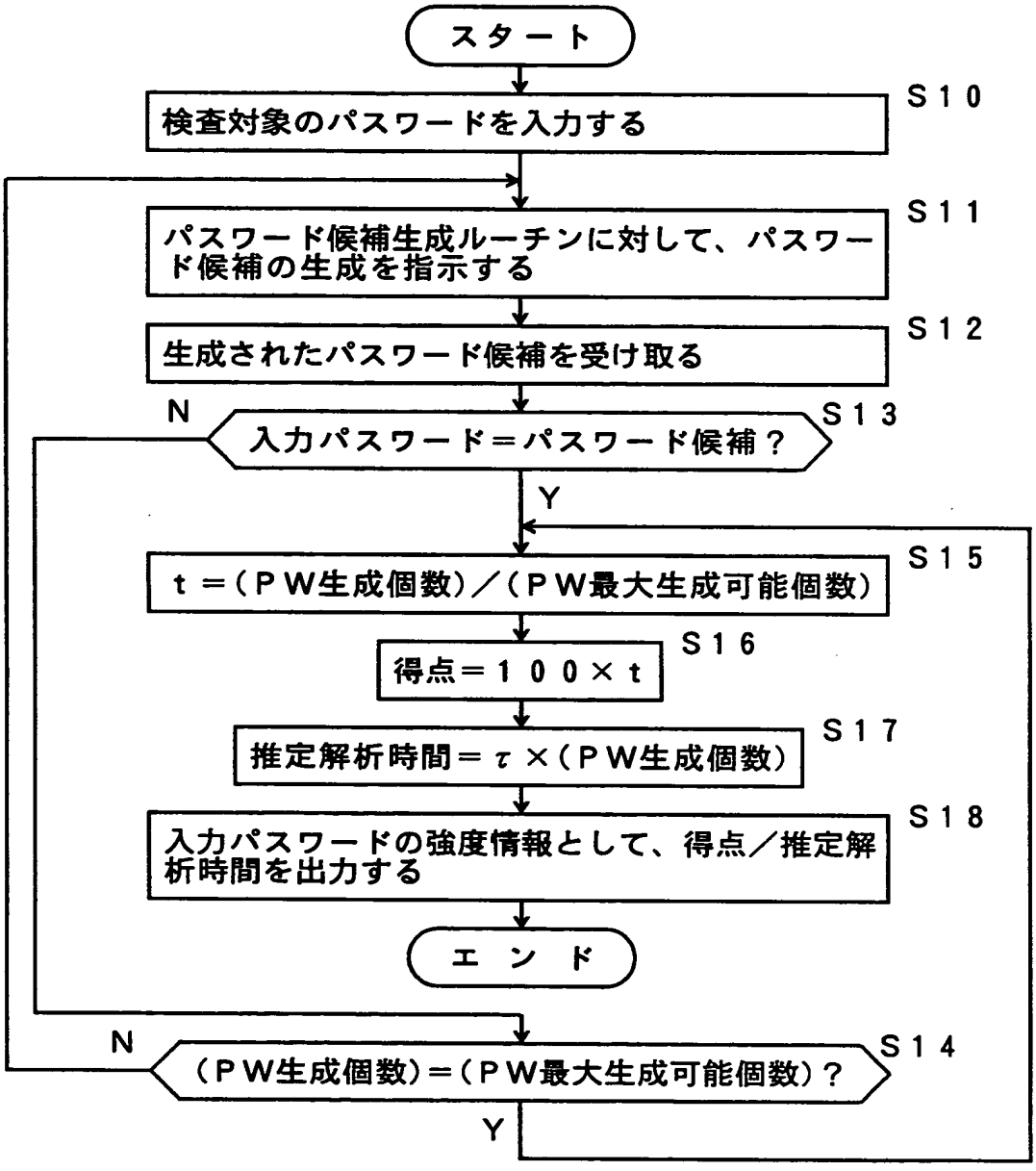
１５　単語辞書

【書類名】　図面

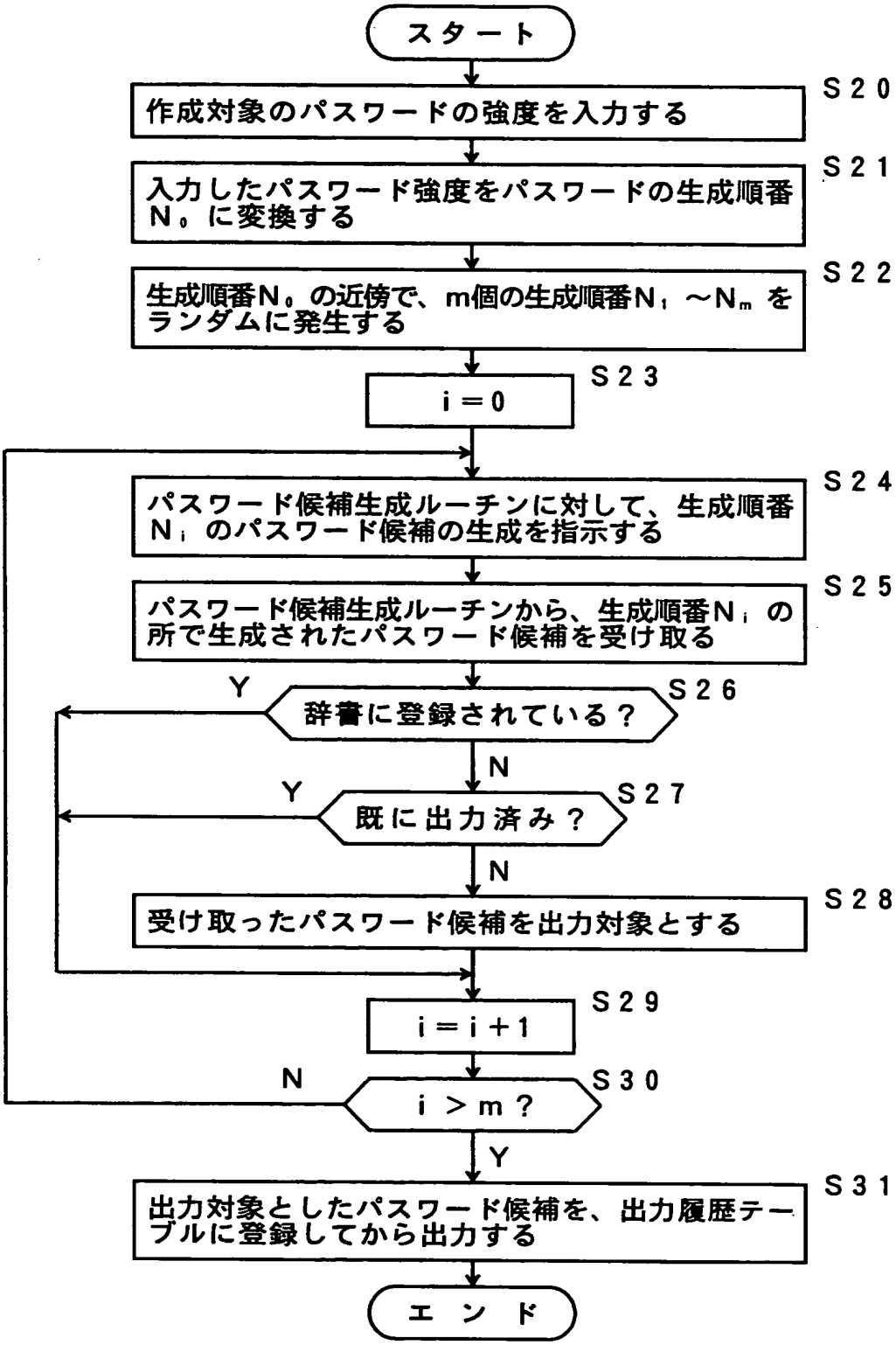
【図１】


1
パスワード作成支援装置
10
入出力装置
11
パスワード候補
生成ルーチン
12
パスワード強度
検査プログラム
13
パスワード作成
プログラム
強度情報入力機能
強度情報変換機能
生成ルーチン制御機能
検索機能
PW出力機能
14
出力履歴テーブル
15
単語辞書
生成要求
パスワード候補
生成要求
パスワード候補
検索
検索

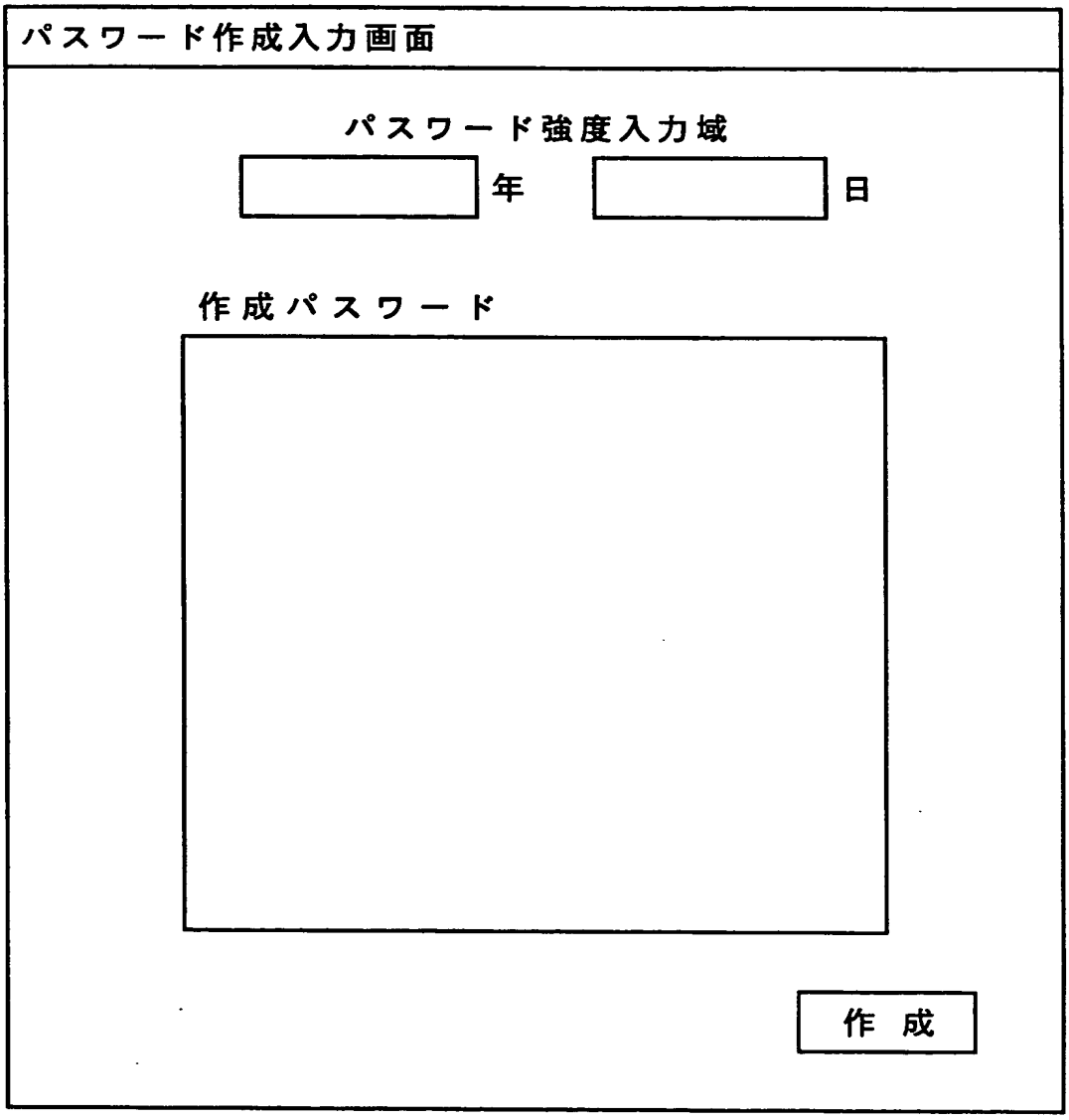
【図２】


スタート
検査対象のパスワードを入力する
S１０
パスワード候補生成ルーチンに対して、パスワード候補の生成を指示する
S１１
生成されたパスワード候補を受け取る
S１２
N
入力パスワード＝パスワード候補？
S１３
Y
t ＝（ＰＷ生成個数）／（ＰＷ最大生成可能個数）
S１５
得点＝１００×t
S１６
推定解析時間＝τ×（ＰＷ生成個数）
S１７
入力パスワードの強度情報として、得点／推定解析時間を出力する
S１８
エ ン ド
N
（ＰＷ生成個数）＝（ＰＷ最大生成可能個数）？
S１４
Y

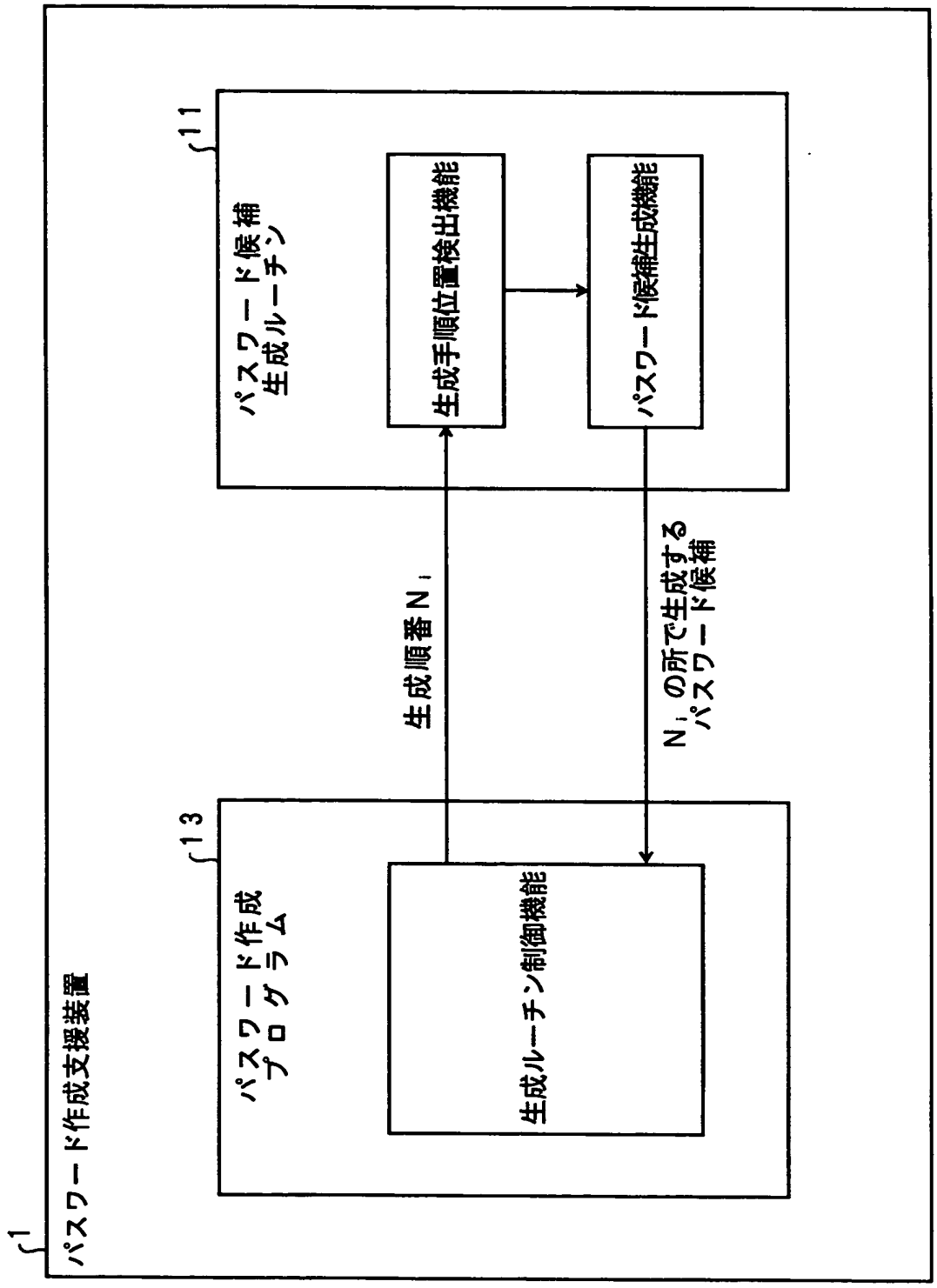
【図３】


スタート
作成対象のパスワードの強度を入力する
S20
入力したパスワード強度をパスワードの生成順番N0に変換する
S21
生成順番N0の近傍で、m個の生成順番N1～Nmをランダムに発生する
S22
i＝0
S23
パスワード候補生成ルーチンに対して、生成順番Niのパスワード候補の生成を指示する
S24
パスワード候補生成ルーチンから、生成順番Niの所で生成されたパスワード候補を受け取る
S25
辞書に登録されている？
S26
Y
N
既に出力済み？
S27
Y
N
受け取ったパスワード候補を出力対象とする
S28
i＝i＋1
S29
i＞m？
S30
N
Y
出力対象としたパスワード候補を、出力履歴テーブルに登録してから出力する
S31
エンド

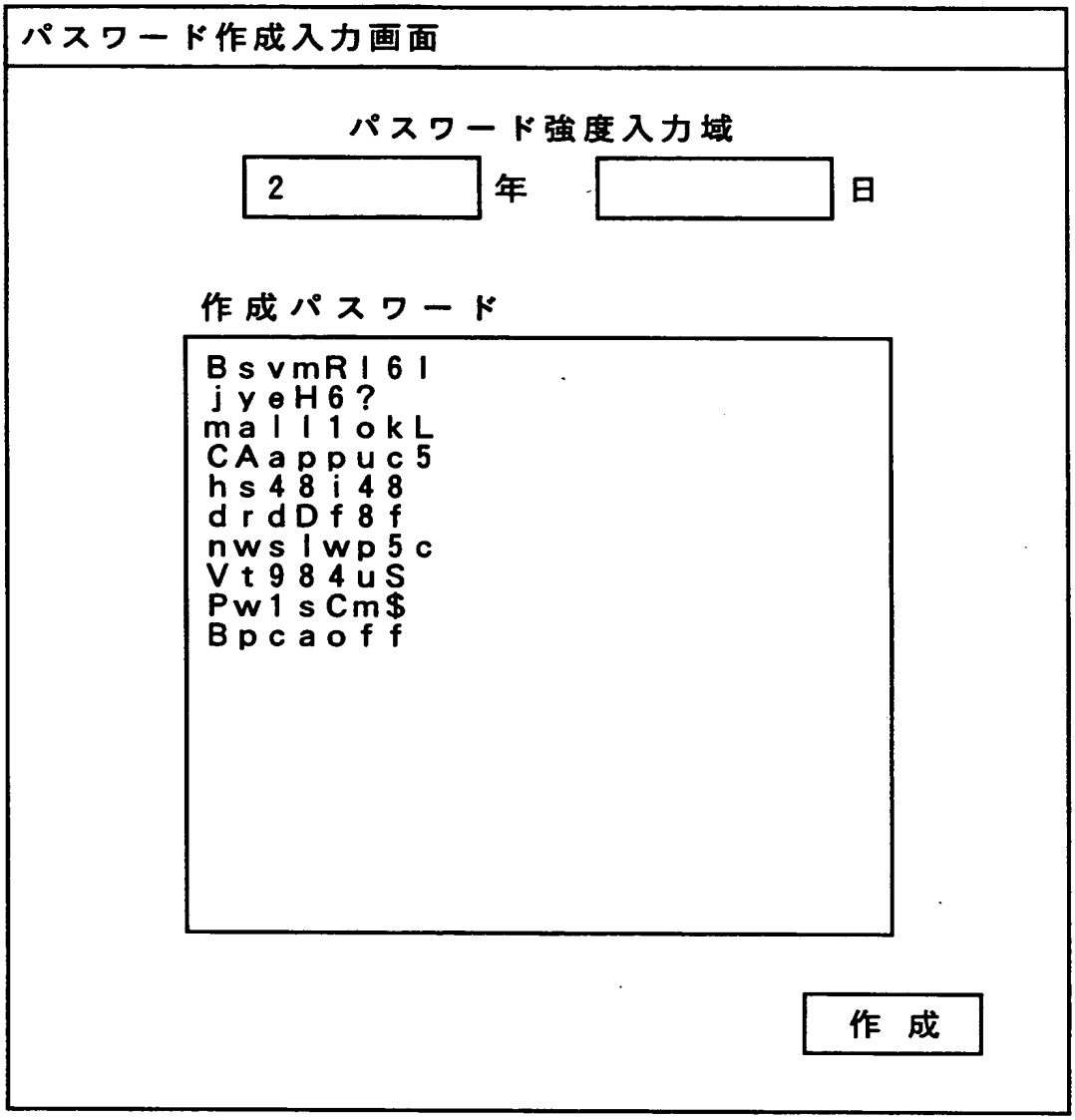
【図４】



【図５】

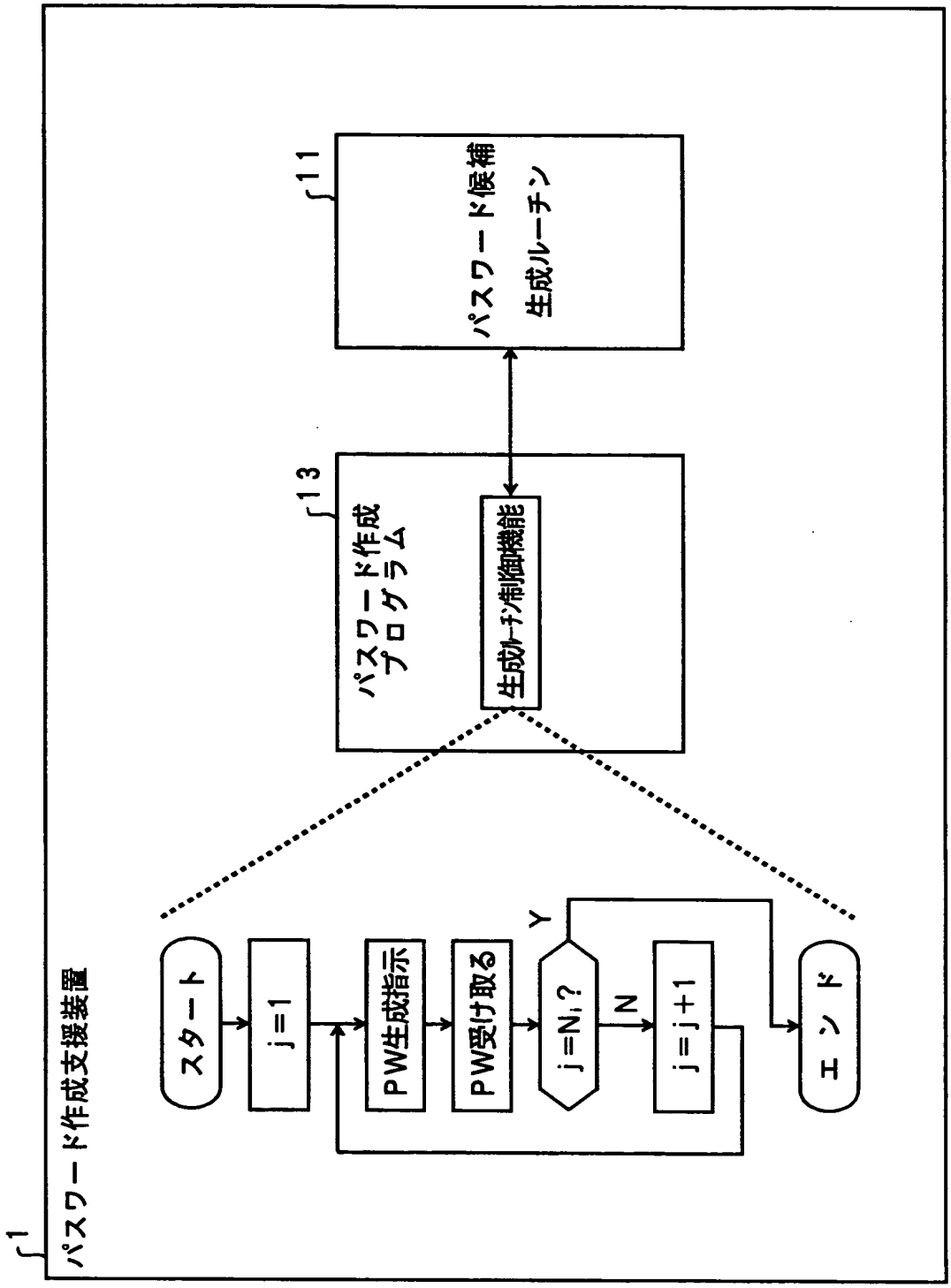

パスワード作成支援装置
1
パスワード作成
プログラム
13
生成ルーチン制御機能
パスワード候補
生成ルーチン
11
生成手順位置検出機能
パスワード候補生成機能
生成順番 N_i
N_i の所で生成する
パスワード候補

【図６】

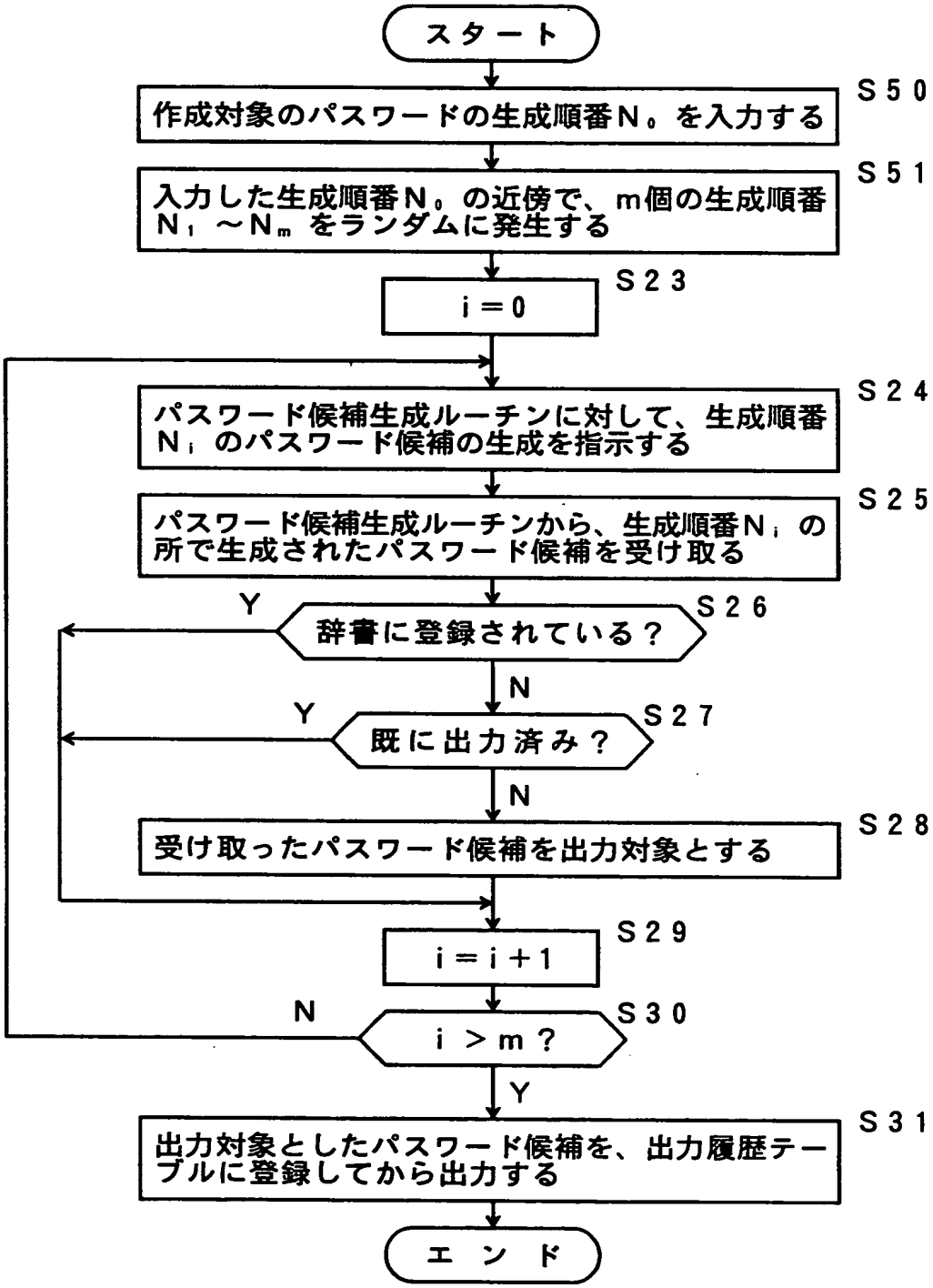


出証特２００３－３０５３４６８

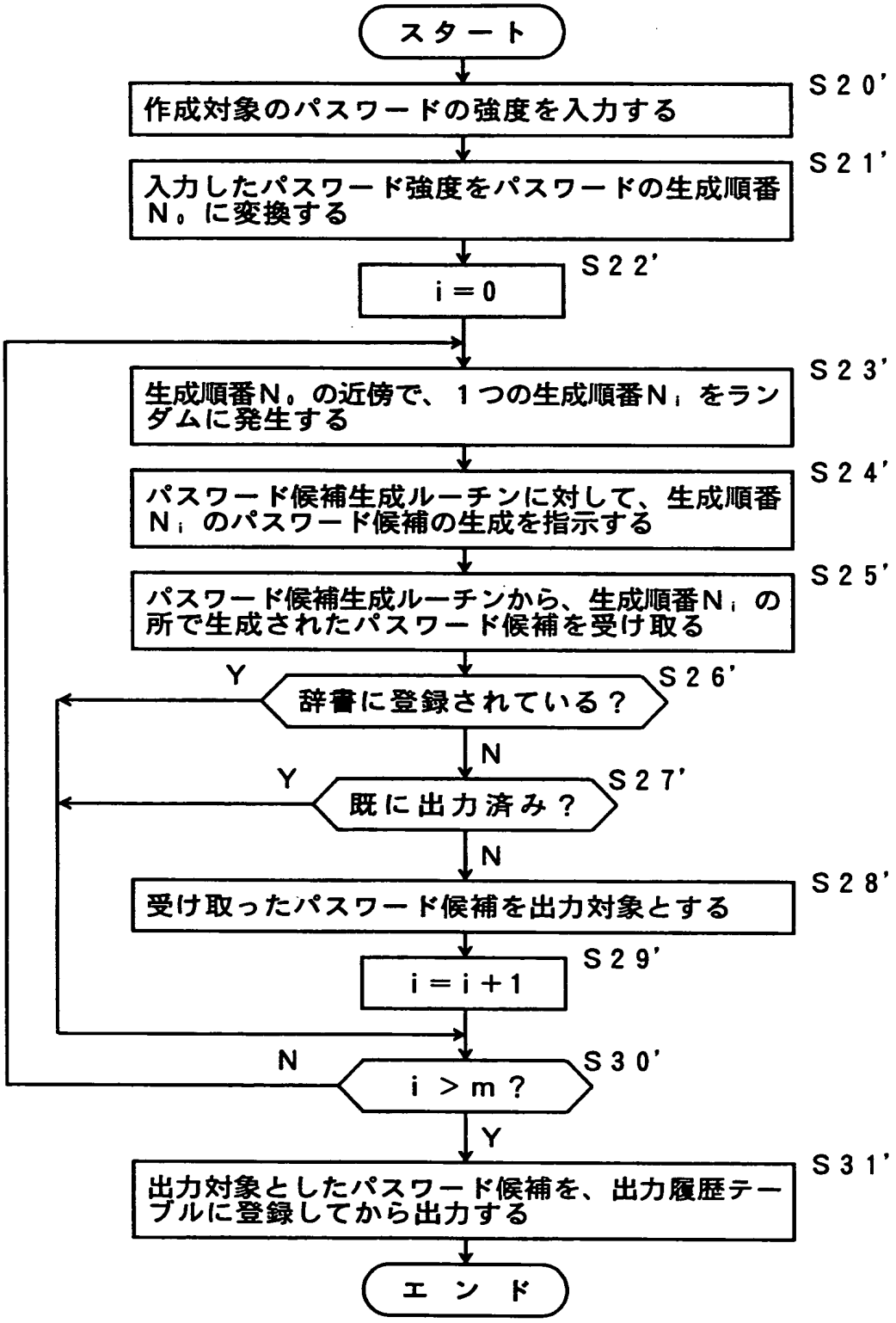
【図７】


1
パスワード作成支援装置
11
パスワード候補
生成ルーチン
13
パスワード作成
プログラム
生成ルーチン制御機能
スタート
j=1
PW生成指示
PW受け取る
j=Ni ?
Y
N
j=j+1
エンド

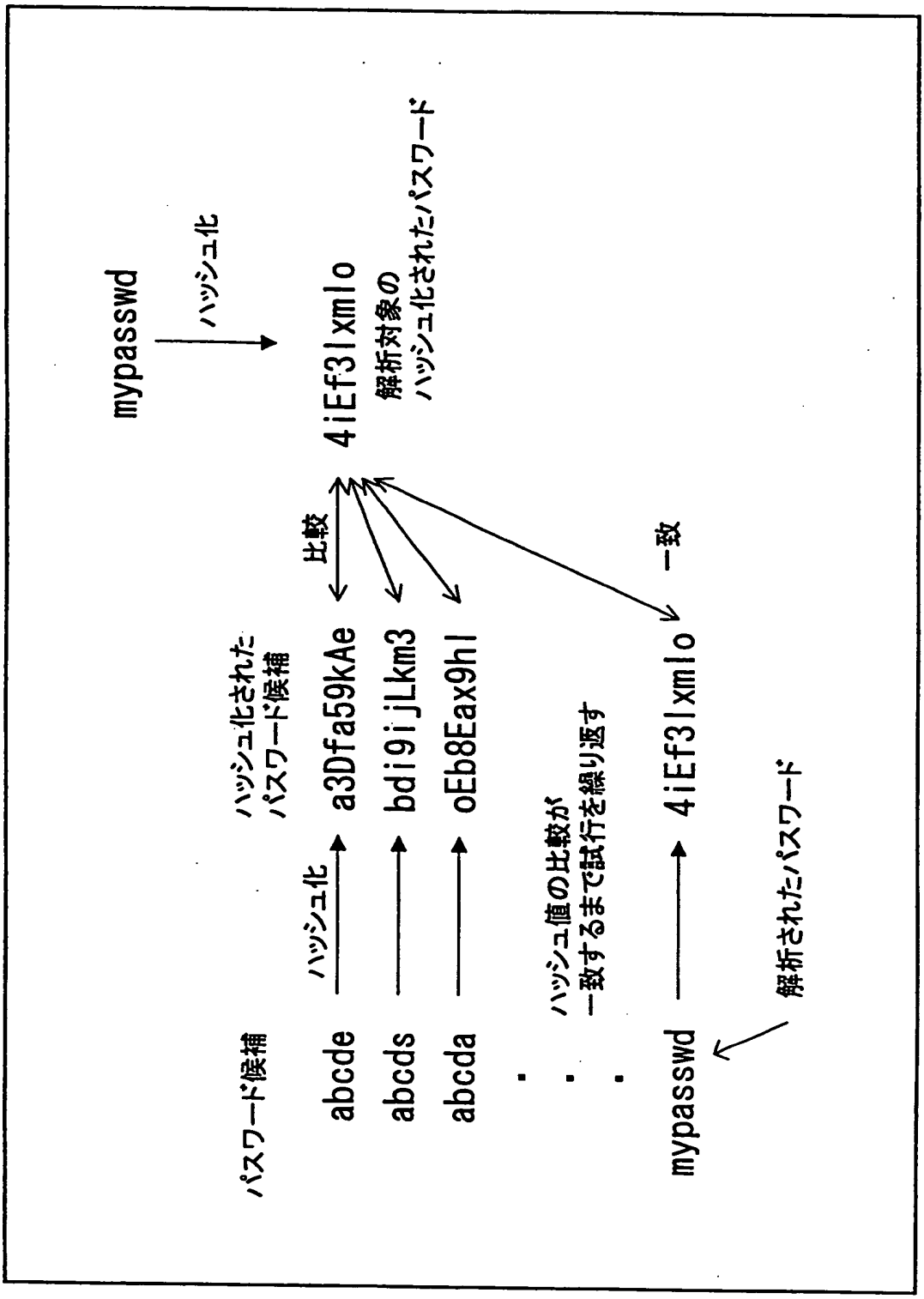
【図８】


スタート
作成対象のパスワードの生成順番N。を入力する
S50
入力した生成順番N。の近傍で、m個の生成順番N₁～Nₘをランダムに発生する
S51
i＝0
S23
パスワード候補生成ルーチンに対して、生成順番Nᵢのパスワード候補の生成を指示する
S24
パスワード候補生成ルーチンから、生成順番Nᵢの所で生成されたパスワード候補を受け取る
S25
Y
辞書に登録されている？
S26
N
Y
既に出力済み？
S27
N
受け取ったパスワード候補を出力対象とする
S28
i＝i＋1
S29
N
i＞m？
S30
Y
出力対象としたパスワード候補を、出力履歴テーブルに登録してから出力する
S31
エンド

【図９】


スタート
作成対象のパスワードの強度を入力する
S２０'
入力したパスワード強度をパスワードの生成順番N。に変換する
S２１'
i＝0
S２２'
生成順番N。の近傍で、１つの生成順番Nｉをランダムに発生する
S２３'
パスワード候補生成ルーチンに対して、生成順番Nｉのパスワード候補の生成を指示する
S２４'
パスワード候補生成ルーチンから、生成順番Nｉの所で生成されたパスワード候補を受け取る
S２５'
Y
辞書に登録されている？
S２６'
N
Y
既に出力済み？
S２７'
N
受け取ったパスワード候補を出力対象とする
S２８'
i＝i＋1
S２９'
N
i ＞ m ？
S３０'
Y
出力対象としたパスワード候補を、出力履歴テーブルに登録してから出力する
S３１'
エ ン ド

【図１０】


mypasswd
ハッシュ化
4iEf3lxmlo
解析対象の
ハッシュ化されたパスワード
比較
一致
ハッシュ化された
パスワード候補
パスワード候補
ハッシュ化
a3Dfa59kAe
bdi9ijLkm3
oEb8Eax9hl
4iEf3lxmlo
abcde
abcds
abcda
mypasswd
ハッシュ値の比較が
一致するまで試行を繰り返す
解析されたパスワード

【書類名】　　要約書

【要約】

【課題】本発明は、強さの保証されたパスワードを作成できるようにする新たなパスワード作成技術の提供を目的とする。

【解決手段】パスワードの強度が、ブルートフォース攻撃に用いられるパスワード推測ツールで生成されるパスワード候補の生成順番に対応付けられることに着目して、ユーザに対して、そのようなパスワードの強度を入力させるようにして、その入力させたパスワードの強度に対応付けられる生成順番を求めて、それに基づいて、パスワード推測ツールを使ってパスワードを作成する。この構成に従って、例えば２年間はブルートフォース攻撃に耐えられるというような強さの保証されたパスワードを作成できるようになる。これから、ユーザは、安心してパスワードを使うことができるようになる。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　　〔０００００６６６６〕

１．変更年月日　　１９９８年　７月　１日
［変更理由］　名称変更
住　所　東京都渋谷区渋谷２丁目１２番１９号
氏　名　株式会社山武